yellowpages: Post-quantum proofs of Bitcoin ownership

Joseph J. Kearney, Conor Deegan, David Nugent & Alex Pruden

May 23, 2025

Abstract

Quantum computing presents an existential threat to Bitcoin. Bitcoin's reliance on elliptic-curve cryptography leaves it vulnerable to quantum adversaries capable of deriving private keys from verification keys; this would give a quantum attacker ownership over the Bitcoin the keys protect. Given Bitcoin's history of slow development and complex governance, coupled with the immense technical challenges associated with upgrading its cryptographic foundations, there is substantial uncertainty over whether Bitcoin can adapt quickly enough to withstand quantum threats. Therefore, off-chain solutions are required to protect user assets before quantum threats become reality.

yellowpages addresses this threat by securely linking users' existing Bitcoin keys to newly generated post-quantum cryptographic keys. This linkage is achieved without publicly revealing the verification keys, preserving existing privacy. Cryptographic proofs of these linkages are registered and timestamped in a publicly verifiable manner, establishing a secure quantum-safe migration path for Bitcoin users. By proactively addressing quantum vulnerabilities independently of Bitcoin's base-layer protocol, yellowpages provides a practical, robust, and scalable safeguard. In the likely case that the Bitcoin core protocol does not upgrade to post-quantum cryptography in time, yellowpages will provide a verifiable proof of accounts that have linked their Bitcoin to a post-quantum key pair. This information can be used to repopulate the Bitcoin blockchain with known, trusted UTXO's. Furthermore, it can be used to facilitate the complex upgrade process facing Bitcoin. This is all done without the user moving or interacting with their tokens on chain.

1 Motivation

Historically, the Yellow Pages served as a trusted directory, connecting people to essential services through publicly accessible records. In a similar spirit but addressing a radically different need, the yellowpages described in this paper acts as a trusted, publicly verifiable cryptographic registry. Instead of connecting users to services, this new yellowpages securely links Bitcoin holders' current

cryptographic identities and holdings to post-quantum (PQ) keys. Just as the traditional Yellow Pages provided critical infrastructure for reliable communication, our version creates an infrastructure for reliable cryptographic migration, ensuring Bitcoin remains secure, trusted, and resilient against the critical threat of quantum computing.

Bitcoin's security is fundamentally threatened by quantum computing. As of the time of writing, Bitcoin has no clearly defined plan to address quantum vulnerabilities inherent in its reliance on elliptic curve digital signature algorithms [1]. Quantum attacks capable of breaking ECC are anticipated within the next decade [2], placing Bitcoin at risk. Such an attack would enable adversaries to forge valid transactions, seize control of user funds and undermine all trust in Bitcoin [3, 4, 5].

Bitcoin's decentralized governance has made cryptographic upgrades exceedingly challenging, with even minor improvements routinely taking significantly longer than originally proposed, leaving the network critically exposed to emerging quantum threats. Notably, major upgrade initiatives have repeatedly missed key deadlines; the Hong Kong Agreement of 2016 and the New York Agreement of 2017 each aimed to implement network upgrades within months, yet both failed to achieve their planned timelines or complete community consensus [6, 7]. The Segregated Witness (SegWit) upgrade, initially proposed in 2015 with broad early support, ultimately took nearly two additional years to activate fully on the network, finally achieving activation in late 2017. Moreover, SegWit's contentious implementation directly resulted in the Bitcoin Cash hard fork, permanently splitting the Bitcoin blockchain and community [8]. Similarly, the Taproot upgrade, despite overwhelming technical consensus since its introduction in early 2018, only became fully activated in late 2021, taking more than three years longer than anticipated to be widely deployed [9].

Without immediate alternative measures, Bitcoin's entire asset base stands vulnerable to quantum compromise, potentially igniting widespread market panic, eroding user confidence, and triggering systemic financial turmoil extending far beyond Bitcoin itself, including critical exposure in institutional investments, retirement pensions, and global financial infrastructure [10]. A proactive, practical solution is therefore not just prudent but imperative, urgently required to safeguard Bitcoin's integrity and preserve trust in the broader digital economy.

The urgency of this solution is underscored by core axioms:

- Practical quantum computing capable of breaking ECC is likely within 10 years [11].
- Bitcoin currently relies exclusively on ECC signatures [12].

- PQ cryptography solutions already exist [13]. They are not yet implemented in Bitcoin.
- Bitcoin's governance structure makes rapid cryptographic upgrades unlikely [9].

yellowpages directly addresses this challenge by enabling Bitcoin users to securely link their current ECC-based keys to newly generated, PQ cryptographic keys. yellowpages achieves this without requiring modifications to Bitcoin's underlying protocol, sidestepping typical barriers to network-wide upgrades.

2 yellowpages Concept

To establish protection via yellowpages, users first generate a PQ verification/private key pair. Users then create a cryptographic proof demonstrating ownership of both their ECC private key and the PQ private key, without revealing the ECC verification key. This proof forms a secure and private link between current Bitcoin holdings and future quantum-safe addresses.

This proof is publicly registered and timestamped within a decentralized registry, creating a transparent, verifiable, and immutable record of PQ ownership. By timestamping this proof before the advent of a CRQC, yellowpages provides verifiable evidence of Bitcoin private key ownership in a post-quantum world.

When quantum threats emerge, yellowpages' pre-established proofs are able to support various practical responses. For instance, wallet providers and exchanges might leverage these proofs to facilitate seamless, PQ migrations for users. Alternatively, the Bitcoin community could utilise yellowpages to inform and streamline a carefully planned upgrade of the Bitcoin core protocol itself. In scenarios where such an upgrade proves impractical or incomplete, yellowpages would serve as a trusted, cryptographically secure foundation to aid the restoration or repopulation of the Bitcoin network. yellowpages' flexibility ensures users have multiple viable options to preserve asset security and network continuity.

3 Creating a Linkage Between Bitcoin and PQ Pairs

Creating a secure, verifiable linkage between existing Bitcoin keys and newly generated PQ-secure keys is fundamental to protecting Bitcoin assets from quantum threats. The cryptographic processes underpinning this linkage are carefully structured into distinct steps, balancing security with practical implementation. This section provides a clear, detailed view of the interactions between the User and the Proving Engine, highlighting how each cryptographic

action contributes to a publicly verifiable yet privately secure linkage.

Creating a cryptographic link between Bitcoin and quantum-resistant keys involves a structured interaction between the User and the Proving Engine. Figure 1 provides a simplified overview of this end-to-end process. Initially, the User generates a quantum-resistant (PQ) key pair and then securely establishes a linkage between their existing Bitcoin address and the newly created PQ address by cross-signing each address with the other's respective private key. The User then provides the Proving Engine with evidence of these signatures, enabling it to verify and cryptographically assert the validity of this linkage without ever exposing sensitive cryptographic information. Finally, the Proving Engine returns a publicly verifiable proof, embedding both addresses within it, establishing an immutable link that is securely recorded and can later be independently verified.

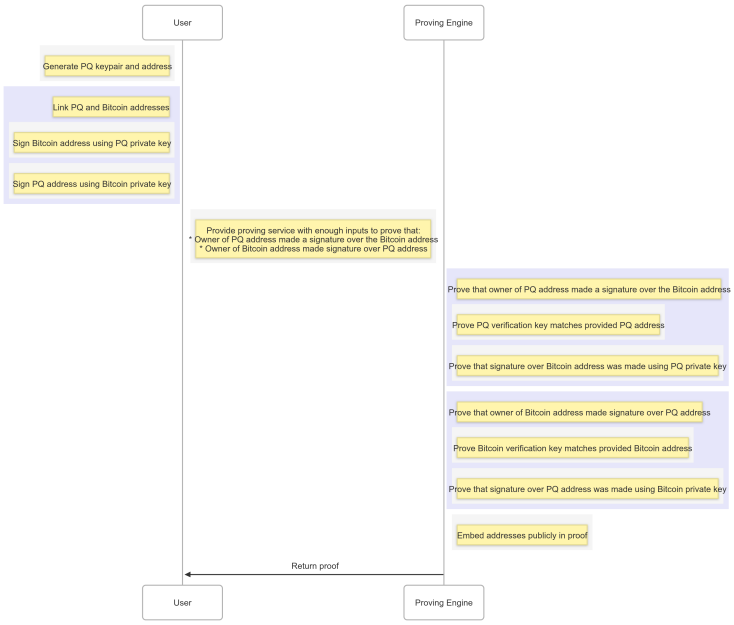

Figure 1: Overview of the cryptographic linkage process, illustrating high-level interactions between the User and the Proving Engine to securely associate Bitcoin addresses with quantum-resistant (PQ) addresses.

From the User's perspective, the process involves clearly defined steps, each securely performed offline, as illustrated in Figure 2. Initially, the User generates a new quantum-resistant (PQ) keypair and computes the corresponding PQ address using the public (verification) key. Next, the User explicitly links their existing Bitcoin and new PQ addresses through a cross-signature process.

Specifically, they sign their Bitcoin address with the PQ private key and separately sign the PQ address using their Bitcoin private key. These mutual signatures cryptographically establish the intended linkage without exposing either private key publicly. Finally, the User provides the Proving Engine with a carefully chosen set of cryptographic inputs, including both verification keys, signed addresses, and the original addresses themselves. This set of inputs enables the Proving Engine to independently verify and publicly assert the legitimacy of this linkage, preparing the cryptographic proof required to secure the User's assets against future quantum vulnerabilities.

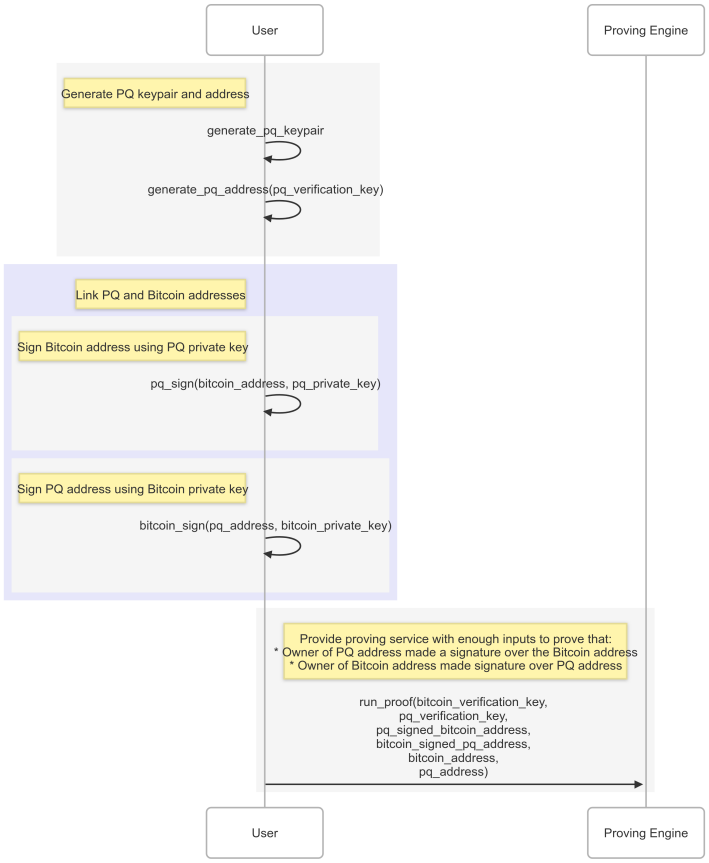

Figure 2: Detailed view of the User's cryptographic steps, highlighting secure PQ key generation, mutual cross-signing of addresses, and preparation of verification data for the Proving Engine

The Proving Engine carries out a rigorous verification procedure to ensure the legitimacy of the cryptographic linkage provided by the User, as depicted in

Figure 3. Upon receiving the inputs, the Proving Engine performs two parallel sets of validations. First, it confirms that the PQ address provided genuinely corresponds to the given PQ verification key and that the signature over the Bitcoin address was created with the associated PQ private key. Next, it independently verifies that the Bitcoin verification key matches the provided Bitcoin address and ensures the signature over the PQ address was indeed generated using the Bitcoin private key. Only after successfully completing these comprehensive cryptographic checks does the Proving Engine embed both addresses into a publicly accessible and verifiable proof, returning this robust proof to the User. These validation steps are critical, as they guarantee cryptographic integrity without compromising user privacy or key security.

By clearly detailing the linkage creation process, yellowpages establishes transparency, cryptographic robustness, and operational simplicity. Each step, from initial key generation to the final proof production, underscores the system's design principles of flexibility, privacy, and independence from Bitcoin's protocol. Through careful delineation of User and Proving Engine interactions, this approach not only mitigates quantum risks but also empowers Bitcoin holders with direct, proactive control over the quantum-resistance of their assets. The full diagram for both the user and the proof engine can be found in Appendix 1.

4 Technical Considerations

The core technical challenge for yellowpages is securely linking existing Bitcoin verification keys with PQ cryptographic keys, without exposing sensitive information. This process must balance quantum-resistance, privacy, efficiency, and practical feasibility. Multiple cryptographic and technological approaches can fulfil these requirements, each presenting distinct strengths and considerations.

4.1 Post-Quantum Cryptographic Keys

Initially, users securely generate a PQ cryptographic keypair, independent of their existing Bitcoin keypair. These PQ keypairs employ algorithms widely recognized for their robustness against quantum threats. Notably, the U.S. National Institute of Standards and Technology (NIST) has standardized three digital signature algorithms (DSAs): ML-DSA (Dilithium), FN-DSA (Falcon), and SLH-DSA (SPHINCS+)[14]. Although these standards represent preferred options, alternative PQ schemes could become viable, underscoring the importance of maintaining flexibility for future selection.

All of these PQ digital signature technologies come with notable performance reductions compared to current ECDSA schemes. Typically, PQ algorithms produce significantly larger key sizes and signatures, which can substantially impact storage requirements and transmission efficiency. Additionally, these schemes

Figure 3: In-depth process of the Proving Engine's validation steps, demonstrating rigorous cryptographic verification and the creation of a publicly verifiable proof embedding both addresses securely.

generally involve greater computational overhead, resulting in increased processing times for key generation, signature creation, and verification operations. Table 1 shows the stark comparison between ECDSA and the current selection

Feature	ECDSA	ML-DSA *(Dilithium)*	FN-DSA *(Falcon)*	SLH-DSA *(SPHINCS+)*
Key Size	∼256 bits	∼2–3 KB	∼1–2 KB	∼20–40 KB
Signature Size	∼512 bits	∼2–5 KB	∼1 KB	∼10–20 KB
Computational Efficiency	High	Moderate–High	Moderate	Low–Moderate

Table 1: Comparison of ECDSA with Post-Quantum Signature Schemes

of PQ algorithms.

4.2 Proof Technology

After securely generating their PQ keys offline, users must prove ownership of their existing Bitcoin keypair. Traditionally, proving ownership involves broadcasting a digital signature which has been signed using the Bitcoin private key; however, this method inherently exposes the verification key through cryptographic signature recovery[15]. In the context of quantum threats, publicly revealing this key is unsafe, as quantum algorithms could subsequently derive the corresponding private key[16]. Therefore, securely demonstrating ownership requires constructing cryptographic proofs that effectively prevent any public exposure of the verification key itself. Two broad approaches can securely facilitate this: Trusted Execution Environments (TEE) and Zero-Knowledge Proof (ZKP) systems. A TEE [17] provides an isolated hardware enclave where remote attestation can be performed, this allows validation of the code running in the enclave[cite]. While TEEs offer mature hardware-based security, they carry implicit trust assumptions regarding hardware vendors and potential vulnerabilities such as Spectre or Meltdown attacks.

Alternatively, ZKP [18] systems, including Succinct Non-Interactive Arguments of Knowledge (SNARKs)[19] and Scalable Transparent Arguments of Knowledge (STARKs)[20], offer purely cryptographic solutions. SNARKs typically produce concise proofs requiring trusted setups; however, their cryptographic soundness property is reliant on assumptions vulnerable to quantum-attacks. STARKs eliminate the need for trusted setups and provide inherent PQ soundness but at the expense of larger proofs and increased computational complexity. Although ZKPs currently seem practical due to their robust cryptographic assurances, selecting between these solutions must carefully consider quantum vulnerability and practical implementation factors. A full table investigating the pros and cons of these technologies can be found in Appendix 2.

4.3 Public Commitment and Timestamping

After securely generating and linking the PQ keypair to their existing Bitcoin keypair, yellowpages must publicly register and timestamp the cryptographic proof. One robust approach involves using a decentralized, censorship-resistant

system such as IPFS, where the proof can be stored publicly, and its cryptographic hash subsequently embedded into the Bitcoin blockchain. Such a method provides verifiable and immutable proof that a user's commitment existed before quantum threats became practical.

While IPFS combined with blockchain timestamping represents a preferred method due to its transparency and resistance to censorship, alternative decentralized storage systems or even purely off-chain solutions may also be viable. Flexibility in this choice will depend on adoption factors, security assurances, and community consensus.

4.4 Technical Criteria for Final Selection

Ultimately, the precise technical decisions guiding the implementation of yellowpages, such as PQ scheme selection, proving technology choice, and storage mechanisms, will be made transparently according to pragmatic criteria outlined clearly here:

- **Quantum-resistance**: Demonstrated resilience against known quantum algorithms.
- **Privacy and Key Confidentiality**: Assurance that Bitcoin verification keys remain secure against quantum attacks and are never publicly exposed.
- **Performance and Scalability**: Practical usability, computational efficiency, and blockchain integration.
- **Transparency and Verifiability**: Clear public auditability of proofs and timestamps.
- **Engineering Maturity and Community Acceptance**: Preference for widely reviewed, tested, and accepted technologies. This involves only using NIST standardised algorithms.

These criteria will inform the iterative implementations of yellowpages, detailed explicitly within future publications, preserving flexibility without compromising the security and practicality envisioned in this whitepaper.

5 Conclusion

The inevitability of quantum computing poses a unique and profound challenge to Bitcoin, threatening the very cryptographic principles on which the system was built. Historical evidence demonstrates that Bitcoin's decentralized governance struggles with timely upgrades, emphasizing the critical need for alternative solutions that bypass protocol-level inertia. The urgency of the quantum threat calls for immediate action rather than passive reliance on traditional,

slow-moving governance processes. yellowpages addresses this challenge pragmatically, offering users a secure and immediate means of proactively securing their assets against quantum threats. Instead of merely reacting to quantum developments, it empowers users with cryptographic tools to protect their assets independently—without ever compromising the sensitive cryptographic material at the core of Bitcoin's security model or requiring them to move their assets to a new network or chain. This strategic approach provides optionality and flexibility, supporting various future scenarios, ranging from orderly protocol upgrades to crisis-driven recovery. In summary, yellowpages is not merely a stopgap; it represents a decisive shift towards user empowerment and proactive security management within the Bitcoin ecosystem. Its adoption signals a recognition that Bitcoin's future resilience depends upon independent, flexible, and quantum-aware solutions, capable of adapting seamlessly to evolving cryptographic landscapes. Proactive action today will secure trust, stability, and the enduring strength of Bitcoin, protecting the broader digital economy from imminent quantum vulnerabilities.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, white paper.

[2] M. Mosca and M. Piani, "2021 quantum threat timeline report," Global Risk Institute, Tech. Rep., 2022.

[3] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," pp. 465–467, 2018.

[4] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on bitcoin, and how to protect against them," 2017, arXiv preprint arXiv:1710.10377.

[5] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, p. 100065, 2021.

[6] "What was the new york agreement?" https://calendar.bitbo.io/ny-agreement/, bitcoin Calendar.

[7] L. Shin, "60 bitcoin agreement promises to break impasse; currency jumps in value," https://www.forbes.com/sites/laurashin/2016/02/21/60-bitcoin-agreement-promises-to-break-impasse-leads-to-jump-in-value/, 2016, forbes.

[8] C. Pérez-Solà, S. Delgado-Segura, and G. Navarro-Arribas, "Analysis of the segwit adoption in bitcoin," in *RECSI 2018*, 2019.

[9] J. Swambo, "Evolving bitcoin custody," 2023, arXiv:2310.11911.

[10] OECD, "Institutional investors and cryptoassets," 2022.

[11] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," 2018, arXiv:1804.00200.

[12] I. Stewart, P. Krysiuk, M. Manulis, and A. Herzog, "Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack," *Royal Society open science*, vol. 5, no. 6, p. 180410, 2018.

[13] N. Sood, "Cryptography in post-quantum computing era," 2024, sSRN.

[14] N. I. of Standards and Technology, "Nist ir 8545: Status report on the fourth round of the nist post-quantum cryptography standardization process," U.S. Department of Commerce, Tech. Rep., 2025.

[15] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Łukasz Mazurek, "On the malleability of bitcoin transactions," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, vol. 8975. Springer, 2015, pp. 1–18.

[16] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE, 1994, pp. 124–134.

[17] V. Costan and S. Devadas, "Intel sgx explained," IACR Cryptology ePrint Archive, Tech. Rep., 2016.

[18] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, 1989.

[19] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," in *USENIX Security*, 2014.

[20] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," 2018, arXiv:1807.11479.

A Full User and Proving Engine Flow

The complete interaction process between the User and the Proving Engine, illustrated in Figure 4, details every step necessary to establish a secure, cryptographic linkage between existing Bitcoin addresses and newly generated quantum-resistant addresses. The User initiates the process by securely generating a PQ keypair and subsequently creating mutual signatures, signing their Bitcoin address with the PQ private key, and conversely, signing the PQ address with their Bitcoin private key. These carefully performed cryptographic operations occur

offline, preserving key confidentiality throughout.

The Proving Engine then rigorously validates the provided signatures and corresponding addresses. It independently regenerates the addresses from the verification keys, confirming their authenticity and ensuring the integrity of the mutual signatures. Once all cryptographic checks are successfully completed, the Proving Engine compiles these results into a publicly verifiable cryptographic proof. This comprehensive process ensures that Bitcoin assets remain securely linked to quantum-resistant keys without compromising private cryptographic material, establishing both transparency and robust protection against future quantum threats.

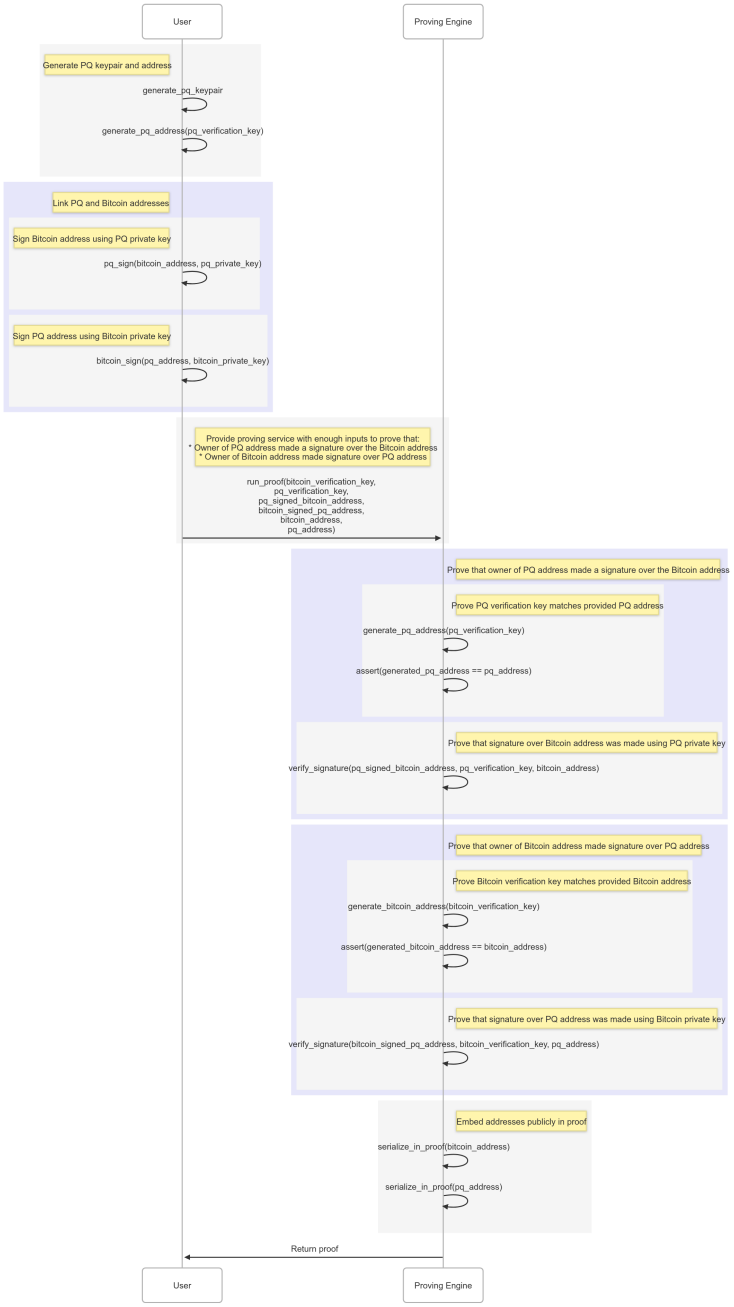

Figure 4: Complete sequence diagram depicting all interactions and cryptographic validation steps performed by the User and the Proving Engine to securely establish a linkage between Bitcoin and PQ addresses

B Zk-STARK, ZK-SNARK and TEE Analysis

Table 3 provides a comparative overview of potential technologies suitable for securely proving Bitcoin ownership without revealing sensitive verification keys. It highlights critical trade-offs between security assumptions, quantum resistance, privacy guarantees, computational efficiency, and practical feasibility. TEEs offer strong hardware-based isolation but introduce centralization risks due to reliance on hardware vendors. Conversely, ZKP systems, specifically SNARKs and STARKs, offer cryptographic trust minimization. SNARKs are efficient but their soundness relies on quantum-vulnerable cryptographic assumptions, while STARKs provide inherent quantum resistance and transparency at the expense of computational overhead and complexity. This summary underscores the importance of selecting technologies that align with both immediate needs and future-proofing requirements.

Table 2: Comparison of ZK and TEE Technologies

Technology	**Privacy**	**Post-Quantum Soundness**	**Scalability**	**Trust Assumptions**	**Limitations**
ZK-STARKs	Not inherently zero-knowledge (requires extra techniques)	Yes (hash-based; avoids algebraic assumptions)	Highly scalable: linear proving, sublinear verification	No trusted setup required	Large proof sizes; slower verification than SNARKs
ZK-SNARKs	Fully zero-knowledge by default	No (relies on Discrete Logarithm; broken by quantum)	Efficient: small proofs, fast verification	Requires trusted setup (initial ceremony)	Breaks after Q-Day; depends on secure setup
TEEs	Privacy within secure enclave execution	No (relies on hardware trust, not cryptography)	Low computational overhead	Trust in hardware vendor (e.g., Intel SGX, AWS Nitro)	Susceptible to side-channel attacks and vendor centralization

Table 3: Comparison of cryptographic techniques for securely linking Bitcoin and quantum-resistant keys, evaluating trade-offs in security assumptions, quantum resistance, privacy properties, and practical deployment considerations.